

Electronic Signature Policy

1. Introduction

- a. Clark County has adopted this Electronic Signature Policy to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Department Health and Human Services (“DHHS”) security and privacy regulations, and the Joint Commission on Accreditation of Healthcare Organizations (“JCAHO”) accreditation standards, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements.
- b. All personnel of Clark County must comply with this policy. Familiarity with this policy and demonstrated competence in the requirements of the policy are an important part of every employee’s responsibilities.

2. Policy

- a. All persons authorized to authenticate medical records must read, understand, and comply with this policy.
- b. In accordance with legal and accreditation standards, Clark County permits practitioners to authenticate entries by executing an electronic signature.
- c. The applicable department or committee is responsible for developing procedures for determining what individuals are authorized to authenticate particular portions of patient medical records. The clinician placing the electronic signature into the specified field(s) is considered to have signed and authenticated that specified information entered into the system as a part of the patient’s legal medical record.
- d. Clark County provides the clinical staff training and orientation on the use of the electronic signature as a required part of training on the automated medical record.
- e. The signature applied is considered the authentication of the specific entry into the medical record, whether that electronic signature image is reviewed on a workstation within the computerized medical record system or whether the signature image has been printed on the paper version of the visit note or medical record entry.
- f. Clinician staff applying the electronic signature are attesting to having reviewed the contents of that entry and having determined that the entry contains what the individual clinician intended. Corrections to an entry must be made by generating a new entry.
- g. To safeguard against unauthorized access to the system and forgery of electronic signatures, the following rules apply:
 - 1) Workstations are locked with password protection.
 - 2) Each individual clinician is assigned an unique ID and password to access to applicable programs.

- h. The department head maintains the assignment of logins and passwords. Only specifically designated staff may perform those tasks under the supervision of the system administrator in accordance with Clark County's Security Policy.
- i. Medical record entries that are locked can be unlocked only by the department head and only in specific circumstances for corrections not related to the content of the medical record, and such unlockings of the medical record are recorded in the audit trail records.
- j. The system may maintain an audit trail providing details of user names accessing medical records and/or unlocking medical records.
 - 1) Clark County will maintain hardware, server, and network security consistent with its Security Policy.
- k. Clark County will train and educate staff in the proper use of the electronic signature.
- l. All clinical staff using the pen-based units (if applicable) for patient documentation must attend security training on the unit, protection of confidential data, and maintaining closed access to the unit. Remote access to the unit is not permitted.
- m. Clark County will instruct clinical staff on the facility's progressive disciplinary policy and that failure to adhere to all required security processes will result in disciplinary action.
- n. Only specific clinical staff have access rights to make an electronic signature entry into a secured area of a patient medical record. Support staff and administrative staff logins do not permit them access to entering or altering electronic signatures or patient data in the system.